ІНФОРМАЦІЙНА БЕЗПЕКА

УДК 681.3

А.О. Ігнатович, Н.Я. Павич
(*Національний університет "Львівська політехніка",*

МОДЕЛІ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТА НАДІЙНОСТІ БЛОКОВИХ ШИФРІВ

За результатами аналізу особливостей та характеристик відомих блокових шифрів запропоновано моделі підвищення їх ефективності та надійності на основі статичного та динамічного включення маскуючих символів. Обґрунтовано підвищення ефективності та надійності блокових шифрів.

Ключові слова: модель, блоковий шифр, ефективність, надійність, маскуючий символ

А.А. Игнатович, Н. Я. Павич

МОДЕЛИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ И НАДЕЖНОСТИ БЛОЧНЫХ ШИФРОВ

По результатам анализа особенностей и характеристик известных блочных шифров предложены модели повышения их эффективности и надежности на основе статического и динамического включения маскирующих символов. Обоснованно повышение эффективности и надежности блочных шифров.

Ключевые слова: модель, блочный шифр, эффективность, надежность, маскирующий символ

A. A. Ignatovich, N. Ya. Pavich

MODES FOR IMPROVING EFFICIENCY AND RELIABILITY OF BLOCK CIPHERS

This research work proposes models of efficiency and reliability increasing of the certain block ciphers. The proposed models are based on the basis of static and dynamic inclusion of masking symbols. Also the analysis of effectiveness of the certain block codes is done. Increasing of block ciphers' strength and effectiveness is justified.

Key words: model, block cipher, efficiency, reliability, masking symbol

Вступ. На сучасному етапі розвитку криптографії ефективність та надійність шифрів є одними із основних показників. Шифрування та дешифрування інформації найчастіше виконуються із використанням обчислювальної техніки, що суттєво розширює їх функціональні можливості. Необхідно також завжди враховувати, що шифрований текст може отримати зловмисник і буде використовувати засоби обчислювальної техніки. Ефективність криптосистеми (алгоритм шифрування та дешифрування, або шифр) визначається трудомісткістю і часом, який затрачається на шифрування та дешифрування повідомлення. Надійність криптосистеми визначається часом, який зловмисник затратить для того щоб розкрити алгоритм шифрування та дешифрування і знайти ключ шифру. Очевидно, що оптимальні ефективність і надійність забезпечити одночасно трудно – ідеальних шифрів не існує. Необхідно знаходити компромісні рішення та врахувати, що часто є конкретні ситуації, які диктують певні ви-

моги до криптосистеми. Наприклад, біржова інформація перестає бути таємною через пару десятків хвилин, але мусить бути зашифрована і передана за лічені секунди. А іноді інформація повинна зберігатися десятиліттями, зате немає вимог до швидкості шифрування.

Огляд літературних джерел. Блокові шифри мають давню історію застосування. До класичних блокових шифрів можна віднести шифр Хілла [1,2] та шифр Віженера [3]. Ці шифри відносять до ручних і їм приписують багато недоліків: примітивні, неефекетивні, ручні. Характеристики блокових шифрів досліджували відомий вчений Клод Шеннон [4] та вітчизняні вчені [5,6]. Шифр «мережа Фейстеля» – це сучасний комп'ютерний шифр, його переваги та недоліки відомі [5,6]. Аналіз літературних джерел показує, що функціональні можливості блокових шифрів не вичерпані. Дослідження стосовно підвищення ефективності та надійності блокових шифрів є обґрунтованими та доцільними.

Постановка задачі дослідження. Дослідити особливості та характеристики відомих блокових шифрів та запропонувати моделі підвищення їх ефективності та надійності

Основні результати дослідження

Розглянемо блокові шифри з точки зору ефективності та надійності. До блокових відносяться такі шифри, в яких за один період шифрування перетворюється певна кількість символів в блоку – ***k***. До найбільш поширених блокових шифрів відносять шифри Хілла та Віженера [1-3,5,6], тому дослідження зосереджені саме на цих шифрах. Шифрування та розшифрування інформації можна подати такими процедурами.

$\mathbf{C_i = A * B_i}$ – процедура шифрування інформації, де C_i - матриця-стовпчик i-того блоку шифрованого тексту; A – матриця-ключ для шифрування інформації; B_i – матриця-стовпчик ***i***-того блоку відкритого тексту;

$\mathbf{B_i = A^{-1} * C_i}$ – процедура розшифрування інформації, де B_i – матриця-стовпчик ***i***-того блоку відкритого тексту; A^{-1} - обернена матриця-ключ для розшифрування інформації; C_i - матриця-стовпчик ***i***-того блоку шифрованого тексту.

Ключем для шифру Хілла є матриця, яка представляється словом, чи довільним набором букв. Для шифрування може використовуватися числова квадратна матриця (3x3, 4x4, 5x5, 6x6,...). Матриця повинна мати обернену матрицю, щоб була можлива операція розшифрування.

Відомий спосіб шифрування інформації Віженера [3,5,6] на основі поліалфавітних перетворень елементів відкритого тексту (ВТ). Суть цього способу полягає в заміні кожного елемента ВТ на елемент шифрованого тексту (ШТ) згідно з буквою ключа, причому для кожної букви ключа є відповідний алфавіт заміни елементів ВТ. Якщо довжина ключа менша за довжину ВТ, то ключ повторюється стільки разів, щоб весь масив ВТ мав певний елемент ключа для перетворення.

Недоліком цьоого способу для шифрування інформації є те, що при великих обсягах ВТ можна знаходити повторення в ШТ, які будуть розташовуватись на віддалях кратних довжині ключа ***k***.

Спосіб шифрування на основі шифру Хілла – поліграмний блоковий шифр підстановки, заснований на лінійній алгебрі. Цей спосіб шифрування давав можливість зашифровувати більш ніж три символи за один цикл. Щоб розшифрувати повідомлення, необхідно звернути шифротекст назад у вектор і потім просто помножити на обернену матрицю ключа.

Необхідно обговорити деякі складнощі, пов'язані з вибором шифрувальної матриці. Не всі матриці мають обернену. Матриця буде мати обернену в тому і тільки в тому випадку, коли її детермінант не дорівнює нулю і не має спільних дільників з основою модуля. Таким чином, якщо ми працюємо з основою модуля 26, то детермінант повинен бути ненульовим і не ділитися на 2 і 13. Якщо детермінант матриці дорівнює нулю або має спільні дільники з основою модуля, то така матриця не може використовуватися в шифрі Хілла, і повинна бути обрана інша матриця (в іншому випадку шифротекст буде неможливо розшифрувати). Тим не менш, матриці, які задовольняють вищенаведеним умовам, існують в достатку.

Шифрування. Для кожної букви латинського алфавіту є відповідне їй число : A = 0, B = 1, ..., Z = 25. Блок з n букв представляється як n-мірний вектор і множиться n × n матрицю по модулю 26 (якщо використовується число більше 26, то можна використовувати іншу числову схему і добавити розділові знаки.) Матриця є ключем шифру. Матриця повинна мати обернену матрицю, щоб була можлива процедура розшифрування.

В наступних прикладах використовуються латинські букви від A до Z, відповідні їм числові значення наведені в таблиці.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Розглянемо процес зашифрування слова 'BCD' з допомогою ключа (GYBNQKURP у буквеному зображені) і відповідному числовому зображені у вигляді матриці розміром 3x3:

$$\begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix}$$

Оскільки букві 'B' відповідає число 1, 'C' — 2, 'D' — 3, то повідомлення можна представити як матрицю стовпець (або вектор):

$$\begin{vmatrix} 1 \\ 2 \\ 3 \end{vmatrix}$$

В цьому випадку зашифрований вектор буде:

$$\begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 2 \\ 3 \end{vmatrix} = \begin{vmatrix} 57 \\ 75 \\ 99 \end{vmatrix} = \begin{vmatrix} 5 \\ 23 \\ 21 \end{vmatrix} \pmod{26}$$

що відповідає шифрованому тексту 'FXV'. Ми бачимо, що кожна буква ШТ змінилася. Шифр Хілла досягнув дифузії по Шеннону, і n-розмірний шифр Хілла може досягнути дифузії n символів за раз.

Розшифрування. Для того, щоби розшифрувати повідомлення, необхідно перетворити символи шифрованого тексту у вектор и перемножити на обернену матрицю ключа (IFKVIVVMI у буквеному зображені). (Існують стандартні методи обчислення обернених матриць, які широко використовуються у матричному численні.) Обернена матриця в нашому прикладі буде

$$\begin{vmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 10 \end{vmatrix}$$

Якщо перемножити матрицю ключ на матрицю стовпчик ШТ - отримаєм

$$\begin{vmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 10 \end{vmatrix} \cdot \begin{vmatrix} 5 \\ 23 \\ 21 \end{vmatrix} = \begin{vmatrix} 365 \\ 730 \\ 549 \end{vmatrix} = \begin{vmatrix} 1 \\ 2 \\ 3 \end{vmatrix} \pmod{26}$$

Результуюча матриця стовпчик дає можливість відновити символи відкритого тексту 'BCD'.

В новому способі шифрування інформації [7] використовуються маскуючі символи, які встановлюються серед символів відкритого тексту (ВТ), що ускладнює процедуру розпізнавання ВТ при переборі можливих варіантів шифрів і переборі ключів для кожного шифра та приводить до підвищення крипостійкості.

Поставлена задача вирішується тим, що в запропонованому способі шифрування інформації при якому виконують поділ символів відкритого тексту (ВТ) на блоки по **μ** символів у блоку, які утворюють матрицю стовчик, а ключ утворюють з μ^2 кількості символів, які записують як квадратна матриця **μxμ** і символи шифрованого тексту (ШТ) формують в процесі перемноження поблоково матриці стовпчика і квадратної матриці ключа шифрування, які попередньо перетворюють у відповідні числа по модулю **n**, де **n** – кількість символів ВТ, дешифрування щифрованого тексту виконують поділом символів ШТ на блоки (по **μ** символів у блоку) і перемноження матриці стовпчика і квадратної матриці ключа дешифрування, які перетворюють у відповідні числа по модулю **n**, де **n** – кількість символів ВТ, згідно винаходу, перед множенням на матрицю, ключ шифрування у відкритий текст перед і після кожного символу ВТ вставляють додаткові маскуючі символи, причому маскуючі символи на кожному кроці вставляння визначаються найменшою частотою вживання цього символу (з врахунком вставлених маскуючих символів) у відкритому тексті з маскуючими символами, а при дешифруванні вилучають маскуючі символи в такому порядку, як вони вставлялися перед множенням на матрицю ключ шифрування.

Встановлення перед процедурою шифрування перед кожним символом і після кожного символу ВТ додаткових маскуючих символів, причому при довжині блоку шифрування **μ** необхідно вставляти таку кількість маскуючих символів (перед і після символу ВТ) щоби в кожний блок шифрування потрапляв хоча би один символ ВТ. Хоча ця вимога не є критичною для виконання, занадто багато маскуючих символів вставляти недоцільно оскільки досягнення результату може бути при незначному збільшенні кількості символів шифрованого тексту (ШТ). Додаткові маскуючі символи вибираються керованим генератором випадкових чисел таким чином щоби статистичний аналіз ВТ до вставляння і після вставляння маскуючих символів змінювався в сторону рівномірної частоти вживання символів. Генератор випадкових чисел на кожному кроці вставляння символу вибирає такий символ, який має найменшу частоту вживання символів. І ця частота вживання символів визначається на кожному кроці і з кожним кроком частотна характеристика ВТ з маскуючими символами стає все більш рівномірною, що унеможливлює отримання однозначного результату при обробці статистичних параметрів тексту. Маскуючі символи в кожному випадку встановлюються відповідно до вибраного методу. Методів встановлення маскуючих символів може бути багато. Ця процедура є доповнювальною до вибору матриці ключа, тому що без знання цього методу відкритий текст не знаходиться. І тільки повна інформація про метод встановлення маскуючих символів і ключ дає можливість розшифрувати за шифрований текст.

Формування матриць ключів для шифрування і розшифрування виконується так, як в шифрі Хілла. Формат матриць ключа і вектора відкритого тексту для шифрування може бути 2, 3, 4, 5, 6... Зараз немає технічних проблем для апаратного, програмного чи комбінованого способу перемноження матриць розміром 2x2, 3x3, 4x4, 5x5, 6x6, ...

Частоту вживання символів у відкритому тексті (ВТ) також нетрудно визначити з допомогою ***k*** лічильників, які будуть визначати скільки раз вживався кожний символ у ВТ. Таким чином маскуючі символи будуть вставлятися перед і після символів ВТ залежно від частоти вживаності, причому в зворотній залежності. Чим рідше вживається окремий символ ВТ, тим частіше він буде всталятися як маскуючий символ. Якщо підрахунок частот вживання символів здійснювати після кожного циклу вставляння (перед і після окремого символу ВТ), то очевидно, що чим більше циклів вставляння маскуючих символів, тим більш рівномірною буде частотна характеристика вживання символів.

Основними прийомами для розпізнавання способу шифрування, визначення довжини ключа є статистична обробка тексту, яка визначає частоту повторення символів, і повторення групи символів ШТ, що може допомогти визначити довжину ключа. Маскуючі символи, які вставляються перед і після кожного символу ВТ. Їх поцедура вставляння в певній мірі має випадковий характер, і вони фактично стають додатковим шифруючим ключем. Справа в тому, що якщо при перемноженні матриць у матрицю символів ВТ вставляється хоча би один маскуючий символ, то при перемноженні змінюються всі результуючі символи ШТ. Якщо перемножимо матрицю ключ на матрицю вектор ВТ, то отримаєм

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} \bullet \begin{vmatrix} 10 \\ 11 \\ 12 \end{vmatrix} = \begin{vmatrix} 16 \\ 11 \\ 6 \end{vmatrix} \quad (\text{mod } 26)$$

Якщо в матриці вектор ВТ замінимо один символ (11 поміняємо на 5), то отримаєм

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} \bullet \begin{vmatrix} 10 \\ 5 \\ 12 \end{vmatrix} = \begin{vmatrix} 4 \\ 7 \\ 10 \end{vmatrix} \quad (\text{mod } 26)$$

Як бачимо, заміна одного символу у векторі ВТ (11 замінили на 5) призвела до того, що всі інші символи також змінилися. Таким чином введення маскуючих символів навіть у невеликій кількості (наприклад вводиться один маскуючий символ перед символом відкритого тексту при форматі матриці ключа 3х3 і матриця вектор ВТ буде змінена так: один маскуючий символ і два символи ВТ і так буде у всіх блоках шифрування) призведе до кардинальної зміни символів ШТ. І це тільки від введення маскуючих символів. А ще відбувається процедура перемноження матриці ключа на на матрицю вектор ВТ. Таким чином, всі закономірності ШТ (з точки зору статистичних характеристик і методик їх обробки) будуть суттєво змінені.

Особливо великі проблеми при зламуванні коротких текстів, які зашифровані запропонованим способом шифрування, тому що статистика для таких паролів, кодів, умовних команд чи інших кодових слів, які означають режими роботи, і т.п., не відповідає статистиці природньої мови ВТ. Тому, в зв'язку з вищевикладеним запропонований спосіб шифрування має потенційно високі параметри криптостійкості, особливо при використанні його в системах безпеки для збереження конфіденційної інформації.

Шифрування інформації запропонованим способом виконується таким чином. Символи відкритого тексту ВТ доповнюються маскуючими символами в такому порядку. Визначення частоти вживання символів у відкритому тексті (ВТ) також визначається з допомогою k лічильників, які будуть визначати скільки разів вживався кожен символ у ВТ. Ця процедура виконується перед початком вставляння маскуючих символів і після кожного циклу вставляння маскуючих символів. Один цикл – це виконана процедура вставляння маскуючих символів перед і після кожного символу ВТ. Чим рідше вживається окремий символ ВТ, тим частіше він буде всталятися як маскуючий символ. Якщо підрахунок частот вживання символів робити після кожного циклу вставляння (перед і після окремого символу ВТ), то очевидно, що чим більше циклів вставляння маскуючих символів, тим більш рівномірною буде частотна характеристика вживання символів.

Таким чином, відбувається підготовка ВТ до процедури шифрування. Далі виконується поділ символів відкритого тексту з маскуючими символами (ВТ+М) на блоки по $\boldsymbol{\mu}$ символів у блоку, ці $\boldsymbol{\mu}$ символів утворюють матрицю стовчик, а ключ утворюється з $\boldsymbol{\mu}^2$ кількості символів, які записуються як квадратна матриця $\boldsymbol{\mu}$х$\boldsymbol{\mu}$ і символи шифрованого тексту (ШТ) формуються в процесі перемноження поблоково матриці стовпчика і квадратної матриці, які попередньо перетворюються у відповідні числа по модулю $\mathbf{n}$, де $\mathbf{n}$ – кількість символів ВТ. Процедура розшифрування відбувається в зворотньому порядку. Символи ШТ діляться на блоки по $\boldsymbol{\mu}$ символів у блоку і почергово перемножуються на обернену матрицю ключ і отримуєм ВТ+М. Остання дія,

яку необхідно виконати – це з розшифрованого тексту ВТ+М видалити всі маскуючі символи в такому порядку, в якому вони вставлялися і отримаємо ВТ.

Запропонований спосіб шифрування інформації [7] має високі параметри щодо криптостійкості, нескладно реалізується апаратним або програмним, або комбінованим способом.

Шифр Хілла при $\boldsymbol{\mu} = 6$ був реалізований у вигляді механічної шифрувальної машинки, описаній в патенті [2], який виконував множення матриць у форматі 6×6 по модулю 26 з допомогою системи шестерень і ланцюгів.

За необхідності отримання високих параметрів щодо криптостійкості необхідно вставляти достатньо маскуючих символів, кількість яких може в декілька разів перевищувати кількість символів відкритого тексту ВТ. Якщо приймається алгоритм вставляння маскуючих символів: вставляється один маскуючий символ перед кожним символом ВТ і один маскуючий символ після символу ВТ. В цьому випадку ВТ з маскуючими символами буде мати таку конфігурацію: в кожному блоці (якщо $\boldsymbol{\mu} = 3$) буде один маскуючий символ перед символом відкритого тексту, символ ВТ і один маскуючий символ після символу ВТ. Блок має такий вигляд: $\{m_i; v_i; m_i;\}$, де m_i – маскуючий символ, v_i – символ ВТ. Якщо конфігурація ВТ з маскуючими символами буде така, яка розглядалася вище, а $\boldsymbol{\mu} = 4$, тоді перший блок буде мати такий вигляд $\{m_i; v_i; m_i; m_i;\}$, другий - $\{v_i; m_i; m_i; v_i;\}$, третій - $\{m_i; m_i\, v_i; m_i;\}$, четвертий - $\{m_i; v_i; m_i; m_i\}$, а пятий буде такий як перший і весь цикл з періодом чотири буде повторятися. Якщо приймається алгоритм вставляння маскуючих символів: вставляється два маскуючі символи перед кожним символом ВТ і нуль маскуючих символів після символу ВТ при $\boldsymbol{\mu} = 3$. В цьому випадку блок має такий вигляд : $\{m_i; m_i; v_i;\}$, де m_i – маскуючий символ, v_i – символ ВТ. Всі блоки будуть мати такий вигляд, тому що кількість вставлених маскуючих символів, які приходяться на один символ ВТ дорівнює $\boldsymbol{\mu}$ -1. Варіантів, які визначають конфігурацію ВТ з маскуючими символами, може бути багато. Вибирати необхідно такі, які забезпечують рівномірність частотної характеристики вживання окремих символів для ШТ. Дослідження частотних характеристик вживання окремих символів ШТ навіть при $m_i = 1$ підтверджує ефективність запропонованого способу шифрування інформації.

Для реалізації нового способу шифрування інформації запропоновані адаптивні моделі встановлення маскуючих символів.

Адаптивність моделі встановлення маскуючих символів можна визначити за алгоритмом їх підбору. Запропоновано маскуючі символи вибирати з можливого набору (відповідає алфавіту повідомлення), які визначаються нерівномірністю частотної характеристики розподілу символів, за принципом: кожний маскуючий символ, який вставляється, повинен покращувати рівномірність частотної характеристики розподілу символів відкритого тексту. Очевидно, що чим більш рівномірний частотний розподіл символів відкритого тексту, тим більш рівномірним буде і розподіл символів шифрованого тексту.

Розглянемо моделі на основі статичного принципу встановлення маскуючих символів - маскуючі символи завжди вставляються у наперед визначені місця відносно символів відкритого тексту. На рис. 1-3 наведені три варіанти статичних моделей встановлення маскуючих символів для формату $\boldsymbol{\mu} = 3$. На графіках m_i – маскуючий символ (пунктирна лінія), v_i – символ ВТ (суцільна лінія), блоки розділені тонкими пунктирними лініями, довжина блоку – 3 символи.

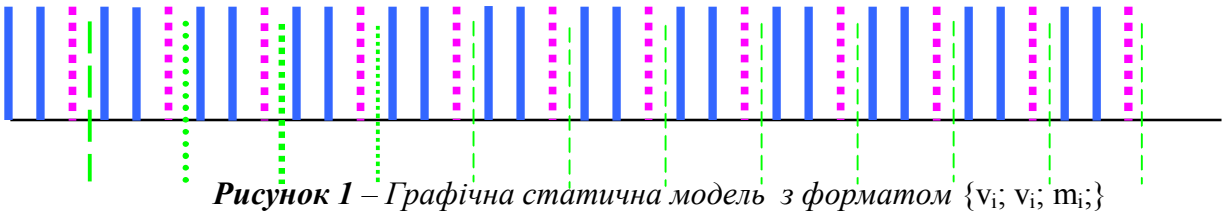

Рисунок 1 *– Графічна статична модель з форматом* $\{v_i; v_i; m_i;\}$

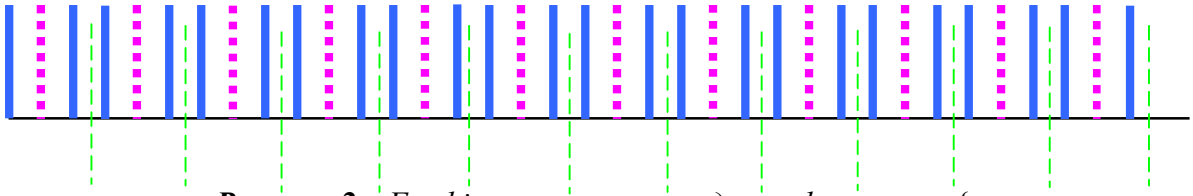

Рисунок 2 *– Графічна статична модель з форматом* $\{v_i; m_i; v_i$

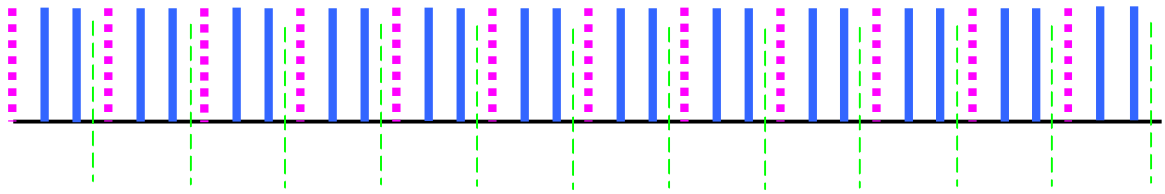

Рисунок 3 *– Графічна статична модель з форматом* { m_i; v_i; v_i;}

Для оцінки ефективності використання маскуючих символів найбільш доцільно використовувати критерій ефективності, в якому оцінюється середнє інтегральне відхилення для конкретного випадку [8]. В наведених на рис. 1-3 моделях формування маскуючих символів для формату **μ** = 3 результат зменшення середнього інтегрального відхилення в 1,4 раза. Такий результат є задовільним і забезпечує підвищення стійкості криптографічної системи [8].

Розглянемо динамічні моделі встановлення маскуючих символів - маскуючі символи вставляються по кількості та на позиції залежно від номера символу відкритого тексту і їх кількість буде змінюватися на кожному етапі процедури вставляння. На рис. 4 наведено приклади динамічних моделей встановлення маскуючих символів для формату **μ** = 5. На рисунках 4 m_i – маскуючий символ (пунктирна лінія), v_i – символ ВТ (суцільна лінія), n_j – коефіцієнт поступово змінюється від 0 до 5 (залежно від порядкового номера символу ВТ v_i). Блоки розділені тонкими пунктирними лініями. Довжина блоку – 5 символів.

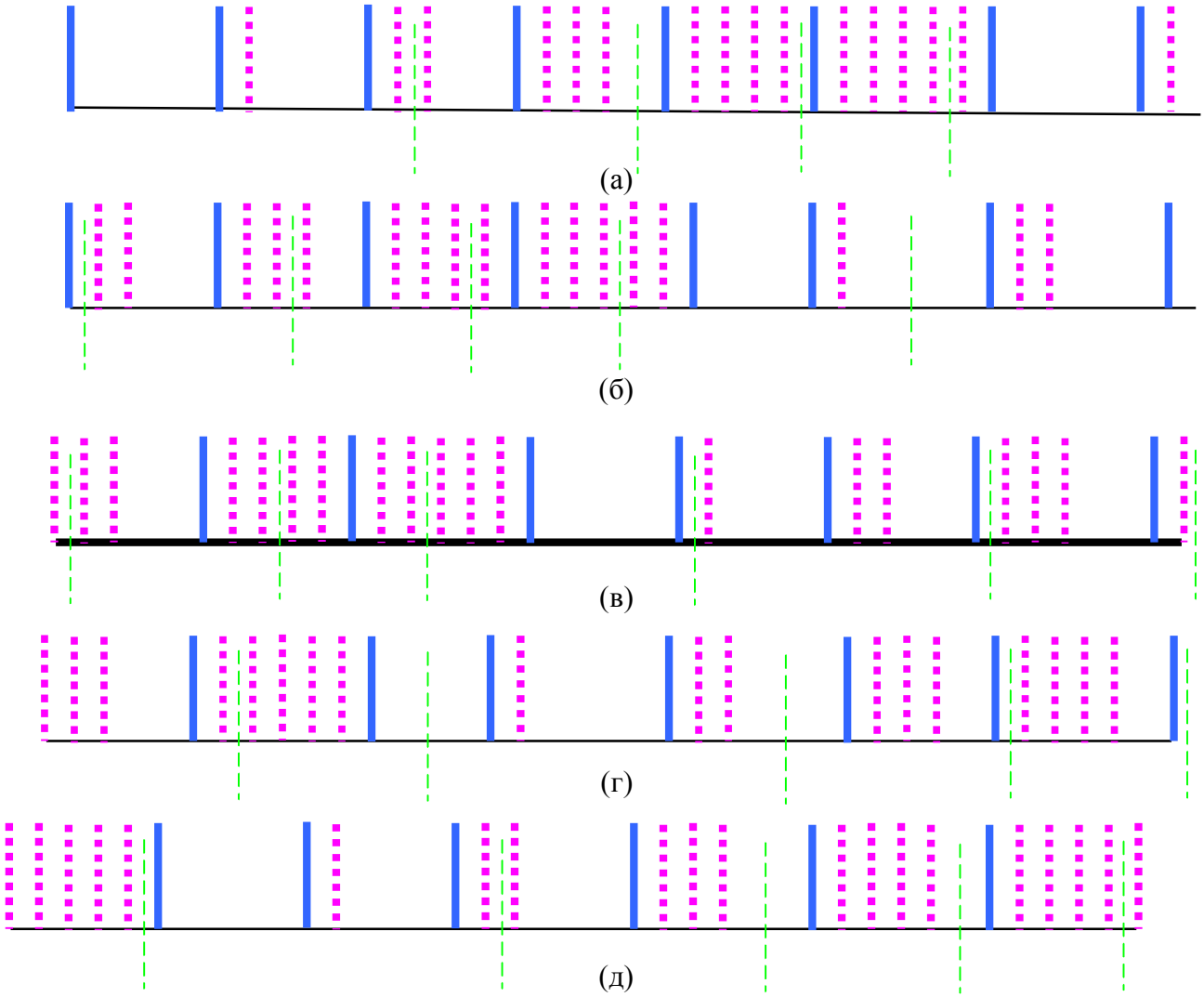

Рисунок 4 *– Графічна динамічна модель з форматом { v_i; n_j*m_i;}*

Динамічна функція вставляння маскуючих символів дає додатковий ефект. Якщо у звичайному шифрі Хілла повторення в тексті можуть появлятися на віддстанях, які кратні довжині ключа (число **μ** не може бути дуже велике), то у встановленні маскуючих символів після кожного символа відкритого тексту у кількості від 0 до 5 при **μ** = 5 період повторення буде 105 символів (замість 5). Саме вставляння маскуючих символів і їх вилучення є процедурою, яка не знижує продуктивність роботи криптографа. При цьому доцільно врахувати, що маскуючі символи підбираються з допомогою генератора випадкових чисел з найменш вживаних символів у шифрованому тексі. Такий алгоритм підбору і маскуючих символів можна вважати додатковим ключем для формування шифрованого тексту. Складність вилучення маскуючих символів не визначається їх номером чи назвою, оскільки вилучаються символи на відповідних позиціях шифрованого тексту. Якщо кількість маскуючих символів більша 50%, тоді частотний розподіл символів у шифрованому тексті наближається до рівноймовірного. Відомий математик Клод Шеннон доказав, що при наближені розподілу частоти вживання символів до рівноймовірного закону, такий шифр наближається до абсолютно стійких шифрів [4]. Таким чином, використання маскуючих символів має перспективу в напрямку створення шифрів підвищеної стійкості.

Якщо раніше вся робота з криптографії виконувалася вручну і було небажано збільшувати довжину ШТ, то при сьогоднішньому стані шифрувальної техніки ця особливість не є визначальною. При використанні шифрувальних машин, спеціалізованих приладів, комп'ютеризованих пристроїв чи комп'ютерів, збільшення ШТ і видалення маскуючих символів виконується достатньо швидко і не зменшує продуктивності праці оператора при шифруванні чи розшифруванні інформації.

Висновки

Результати аналізу особливостей та характеристик відомих блокових шифрів показали можливість підвищення їх ефективності та надійності. Запропоновані моделі на основі статичного та динамічного включення маскуючих символів забезпечують підвищення ефективності та надійності блокових шифрів. Обґрунтовано підвищення ефективності та надійності блокових шифрів. Якщо кількість маскуючих символів становить більша за 50%, тоді частотний розподіл символів у шифрованому тексті наближається до рівноймовірного, що підвищує надійність шифру. Ефективність шифру підвищується завдяки відносно простим алгоритмам шифрування-розшифрування та можливості його реалізації апаратно-програмними комп'ютерними засобами. Запропоновані моделі можуть використовуватися при побудові засобів безпеки комп'ютерних систем, мереж, кібер-фізичних систем.

Список літератури:

1. Lester S. Hill . Cryptography in an Algebraic Alphabet». «The American Mathematical Monthly». – 1929.

2. U.S. Patent 1 845 947. Лестер С. Хілл. Пристрій для шифрування. 1929.

3. Fred Cohen . A Short History of Cryptography // Introductory Information Protection. — 1987. — ISBN 1-878109-05-7.

4. Shannon C. E. Communication Theory of Secrecy Systems // Bell System Technical Journal. – 1949.

5. Вербицький О.В. Вступ до криптології // Видавництво науково-технічної літератури. – Львів, 1998. ISBN 966-7148-03-3.

6. Ємець В. Сучасна криптографія: основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БАК. – 2003. – 144 с.

7. Спосіб шифрування інформації. Патент України на корисну модель №99073. Бюл**.** № 9 від 12.05.2015. Ігнатович А.О., Іванців В. Р., Іванців Р-А. Д., Павич Н. Я.

8. Ігнатович А.О. Критерій ефективності для визначення стійкості блокових шифрівна основі внесених змін статистичних характеристик шифрованого тексту / Ігнатович А.О., Глухова О.В., Лозинський А.Я., Яремчук Р.І. // АСІТ'5 "Сучасні комп'ютерні інформаційні технології". ТНЕУ. – *Тернопіль. 22-23 травня 2015. – С. 167-168.*

References:

1. Lester S. Hill . Cryptography in an Algebraic Alphabet». «The American Mathematical Monthly». – 1929.

2. U.S. Patent 1 845 947. Lester S. Khill. Prystriy dlya shyfruvannya. 1929.

3. Fred Cohen . A Short History of Cryptography // Introductory Information Protection. — 1987. — ISBN 1-878109-05-7.

4. Shannon C. E. Communication Theory of Secrecy Systems // Bell System Technical Journal. – 1949.

5. Verbyts'kyy O.V. Vstup do kryptolohiyi // Vydavnytstvo naukovo-tekhnichnoyi literatury. – L'viv, 1998. ISBN 966-7148-03-3.

6. Yemets' V. Suchasna kryptohrafiya: osnovni ponyattya / V. Yemets', A. Mel'nyk, R. Popovych. – L'viv: BAK. – 2003. – 144 s.

7. SpSpysok literatury:

1. Lester S. Hill . Cryptography in an Algebraic Alphabet». «The American Mathematical Monthly». – 1929.

2. U.S. Patent 1 845 947. Lester S. Khill. Prystriy dlya shyfruvannya. 1929.

3. Fred Cohen . A Short History of Cryptography // Introductory Information Protection. — 1987. — ISBN 1-878109-05-7.

4. Shannon C. E. Communication Theory of Secrecy Systems // Bell System Technical Journal. – 1949.

5. Verbyts'kyy O.V. Vstup do kryptolohiyi // Vydavnytstvo naukovo-tekhnichnoyi literatury. – L'viv, 1998. ISBN 966-7148-03-3.

6. Yemets' V. Suchasna kryptohrafiya: osnovni ponyattya / V. Yemets', A. Mel'nyk, R. Popovych. – L'viv: BAK. – 2003. – 144 s.

7. Sposib shyfruvannya informatsiyi. Patent Ukrayiny na korysnu model' #99073. Byul. # 9 vid 12.05.2015. Ihnatovych A.O., Ivantsiv V. R., Ivantsiv R-A. D., Pavych N. Ya.

8. Ihnatovych A.O. Kryteriy efektyvnosti dlya vyznachennya stiykosti blokovykh shyfrivna osnovi vnesenykh zmin statystychnykh kharakterystyk shyfrovanoho tekstu / Ihnatovych A.O., Hlukhova O.V., Lozyns'kyy A.Ya., Yaremchuk R.I. // ACIT"5 “Suchasni komp"yuterni informatsiyni tekhnolohiyi”. TNEU. – Ternopil'. 22-23 travnya 2015. – C. 167-168.

osib shyfruvannya informatsiyi. Patent Ukrayiny na korysnu model' #99073. Byul. # 9 vid 12.05.2015. Ihnatovych A.O., Ivantsiv V. R., Ivantsiv R-A. D., Pavych N. Ya.

8. Ihnatovych A.O. Kryteriy efektyvnosti dlya vyznachennya stiykosti blokovykh shyfrivna osnovi vnesenykh zmin statystychnykh kharakterystyk shyfrovanoho tekstu / Ihnatovych A.O., Hlukhova O.V., Lozyns'kyy A.Ya., Yaremchuk R.I. // ACIT"5 “Suchasni komp"yuterni informatsiyni tekhnolohiyi”. TNEU. – Ternopil'. 22-23 travnya 2015. – C. 167-168.

❖❖❖